(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number
WO 01/29731 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/28387

(22) International Filing Date: 13 October 2000 (13.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/422,621 21 October 1999 (21.10.1999) US

(71) Applicant: 3COM CORPORATION [US/US]; 5400 Bayfront Plaza, Santa Clara, CA 95052-8145 (US).

(72) Inventors: THOMPSON, Curtis, Duane; 1481 West Bluemont Drive, Taylorsville, UT 84123-6666 (US). CROFT, Kenneth, A.; 2159 South Hannibal Street, Salt Lake City, UT 84106 (US).

(74) Agents: MASCHOFF, Eric, L. et al.; Workman, Nydegger & Seeley, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

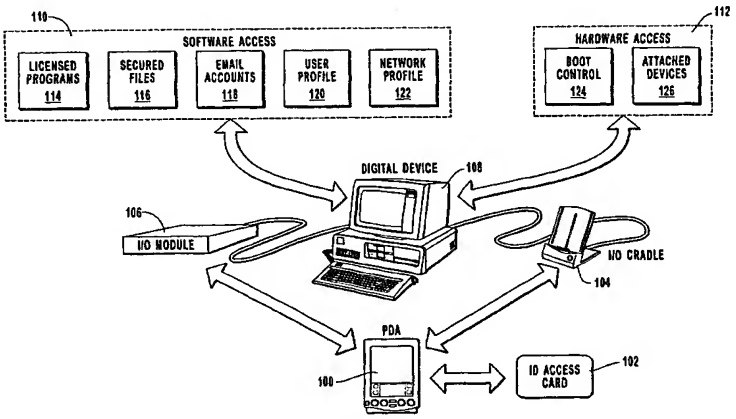
(81) Designated States *(national)*: CN, DE, FI, GB, JP, SE.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ACCESS CONTROL USING A PERSONAL DIGITAL ASSISTANT-TYPE



(57) Abstract: An access control system combining PDA functionality with user authentication so that only the authorized user or users may obtain access control codes from a PDA device for an access control point. The access control point can be a computer terminal (108), a computer file, a door, a checkstand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system attaches to a computer (108) via a PDA cradle (104) and transmits access control codes that include a series of authentication codes or identification codes having encoded data stored within a PDA database. In another form of the invention, user authentication is obtained by comparing biometric data such as a fingerprint with digitally stored data of the authorized user. A decision to grant access affects the release, an electronic release or electronic strike, or electronic software hold. If desired, a write feature can be included into the system whereby each access control point accessed or attempted to be accessed by a PDA user will be recorded on the PDA to determine where access has been attempted. Additional records could be maintained along with the authentication I.D. including checking account information, credit card information, membership information, network information, user profile information (120), e-mail information (118), and personal information.

WO 01/29731 A1

ACCESS CONTROL USING A PERSONAL DIGITAL ASSISTANT-TYPE

BACKGROUND OF THE INVENTION

1. The Field of the Invention

This invention relates to a method for authorizing access control using a PDA device. More particularly, the invention relates to an access control system that uses a PDA device to reference secured data, which thereby facilitates implementation of a selective access policy by a service controller in communication with the PDA device.

2. Description of the Prior Art

One of the challenges of the modern consumer is to maintain a respectable size of their wallet without discarding any required information. As such an individual may be required to carry with their planner, a drivers license, a plurality of credit cards and gas cards, social security numbers, photographs of the family, personal identification, checkbooks, check ledgers, bank account numbers, a telephone list of frequent contacts, various business cards, business notes and other necessities. The net result is a wallet that no longer fits within the constraints of the user's purse or pocket.

Personal Digital Assistant (PDA) devices, like the 3Com PalmPilot®, provide a user with an easy, compact device that can hold all of a user's daily essentials in one place. A PDA device provides a user with quick and easy access to multiple applications customized to meet the individual user's needs. A successful PDA device is lightweight enough to carry everywhere and small enough to fit into a pocket, as a user won't use the PDA device if they don't carry it. Other desirable features found on a PDA device include instant information access, intuitive construction for easy use, conservative energy cell consumption, extensive personal calendaring features, a customized address book, a digital memo pad, an expense calculator, desktop e-mail connectivity, Internet compatibility, and local or remote database synchronization. While the development of PDA devices has dramatically reduced digital complexity for the user, holding thousands of addresses and hundreds of notes or e-mail messages in one portable device, PDA devices have not provided improved access control for the user. Security features in modern PDA devices focus on the data security, data backup, or access security to the specific PDA device. What is needed is a PDA device that provides access control codes to multiple security outlets or service controllers, including access to: desktop computers for boot up, selective computer data or programs, mechanical hardware such as electronic doors, and service identification numbers such as credit card numbers and checking accounts.

The development of new digital device features are driven by the need for the digital device to perform a specific function. As a result, access control issues are virtually a non-existent factor in the overall design of a digital device. Traditionally, physical security may have been present, but the single user nature of early digital devices did not require exhaustive security methods within the digital device itself. While PDA devices continue to operate in predominately single user environments, other digital devices require more emphasis on access control. With the development of multiple user operating systems, segregated work groups containing multiple users, and personalized desktops varying each computer display from one user to the next; access control is a desirable quality for a computer system.

Examples of computer data felt to require access control include secure files, personalized e-mail accounts, specific user profiles, specific network profiles, and access to licensed programs. A secure file may be created by a user encrypting the file with a password. E-mail accounts obtain limited security by archiving data into personalized data structures or by password protecting e-mail access. Access to specific user profiles and network profiles are often controlled by operating system passwords. Many licensed programs require that only a specific quantity of users within a company be granted access and that additional users are not allowed access to these program. This regulation is generally accomplished by either assigning an access control code to each authorized user or the licensed program may regulate a hard quantity limitation on the total number of copies of the program that can be running from a server at any one time. By focusing on access control mechanisms surrounding the files, productivity and efficiency are reduced. These problems are enhanced if an individual user regularly switches work station locations to different access points within the company. Hence, a portable system which provides all file, user, network, or licensing authentication for a particular user would be useful for a corporation in managing its computer usage or license usages and would increase the efficiency and productivity of the user. Not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application.

A variety of access control systems and devices presently exist, however; these access control systems do not interface or coordinate with PDA devices. Specifically, a user attempting to gain access to various resources within a company is often required to carry an access card, an access key, or an I.D. access badge. The user may be required to know an access number, a PIN number, a combination, a password, or to provide a computer authorization number. In addition to these standard electronic and mechanical access control devices, some high security areas require an individual to provide specific

biometric information such as fingerprint verification or a retinal scan. A system that provides all of the necessary access control information using a PDA device as a substitute for the aforementioned keys, cards, or passwords would considerably lessen the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization, not to mention the additional benefit of drastically reducing the extent and magnitude of security access devices necessary for any one individual to carry with them.

Another area presently mired by the excessive numbers associated with access control are commercial transactions for goods or services. Unless a participant is using cash, the service provider or supplier will likely be required to obtain a purchase order number, a credit card, or a check. To complete the transaction, additional physical identification may be required in the form of a drivers license, a passport, a purchase order, a check verification card, or a credit card authorization number. Once again, a system that could maintain these access controls within the parameters of a PDA device would be a marked improvement over the present state of the art.

SUMMARY AND OBJECTS OF THE INVENTION

The foregoing problems in the prior state of the art have been successfully overcome by the present invention which is directed to a system and method for coordinating the production of access control codes by a PDA device to multiple security outlets or service controllers. The system and method of the present invention is scalable in that the PDA device can be adapted to accommodate an unlimited variety of access control codes for a variety of electronic, mechanical, or electrical controllers. Furthermore, the invention allows for the attachment of identification access cards either to program the PDA device to produce the access control codes, to work in conjunction with the PDA device, or to function independent of but attached to the PDA device.

The system and method of the present invention utilize a PDA device to provide improved access control for a user. According to the present invention, a PDA device is programmed to provide various access control codes to multiple security outlets or service controllers, specifically including access codes for: desktop computers during the boot up process, selective secured computer data files, protected or licensed programs, mechanical hardware such as those used with electronic latch doors, and service identification numbers such as credit card numbers and checking accounts.

The present invention supports an access control process that may be summarized as follows. A user enters access control information into a database in order to allow a PDA device to selectively retrieve the information for service controllers or security

outlets. The user may also enter the access control information directly to the PDA device through an interface device. The access control information includes access control codes used to enable the boot-up process for a connected digital device. These codes may also be used to authorize the transfer of funds in a commercial transaction. Access control codes can instruct the PDA device to produce the enabling or disabling signal for an electronic lock on items as diverse as a door and a secured computer file. Just as there are many different types of access control codes, there are multiple methods of delivering the codes to a service controller or security outlet. One method is through the I/O cradle attached to the PDA device and the digital device. I/O cradles are usually attached to either the serial RS-232 port or the parallel port. Another interface method is between a PDA Infra-Red (IR) port and an I/O module attached to the digital device with a IR interface. A preferred embodiment of the present invention utilizes wireless transceiver, built into the PDA device to communicate with a receiver. Finally traditional interface parts, coils, or transmissions may be effectively used. These interfaces include RF, Wegand, magnetic, USB, or laser communication. A final potential embodiment includes integrating an IC chip into the digital device providing access control codes faster.

In one embodiment, the system and method of the present invention provides all the file, user, network, or licensing authentication necessary for a particular user. Once the PDA device is plugged into an I/O cradle, all of the necessary password verification or authentication is supplied by the PDA device. A less memory intensive approach calls for the storage of a solitary password within the PDA access control database which downloads a user profile from a network location. Additional security checks could be implemented to verify that the PDA device holder is the actual user without negatively affecting the efficiency and productivity of the user because of the overall reduction in the number of access control codes. Another embodiment maintains communication between the PDA device and the digital device through an I/O module, such as a wireless transceiver or IR port. If a wireless transceiver is used, the PDA device can download information from the user's workstation at any time or from any location. The wireless PDA device embodiment could alert a user when someone is attempting unauthorized access to the user's computer. Another embodiment utilizes the PDA device to provide the access control codes for a user and then retrieves a customized user desktop setting for the user specified by the PDA device. This feature allows an individual user to attach to any computer within a company's network and obtain their customized desktop. This feature allows for incredible flexibility and versatility, not to mention the added benefit of no longer needing to remember all the passwords used for each "secure" application.

An alternative embodiment accepts access cards, security cards, or hard coded interface devices so that the PDA device may be used as a programmable access control device. The identification access card could be added as a clip-on, or built into the plastic of the PDA device. Access control functionality could even be added using an encoded, integrated circuit added to the PDA device's printed circuit board. The identification access card could utilize a variety of interfaces with the PDA device, including: bar code, USB, IR, laser, Wegand, RF, or magnetic interfaces. The significance of the PDA interface is that external reading is easily accomplished using the PDA device or security card reader. With this versatility, the PDA device may act as either the security device itself or the access control device. Access information is sent out from the I.D. card or from the I.D. card to the PDA device and then from the PDA device itself.

Another embodiment comprising the system and method of the present invention programs a PDA device to act as a substitute for the access keys, cards, combinations, or passwords currently associated with building security. By allowing the PDA device to either provide the authorization codes or the identification information, the security delays and inefficiencies created by the multiple verification devices presently required to obtain site access authorization is drastically lessened, not to mention the additional benefit of drastically reducing the sheer quantity of security access devices necessary for any one individual to carry with them.

Yet another embodiment of the system and method of the present invention allows the PDA device to present the access control numbers associated with commercial transactions for goods or services. A properly programmed PDA device can provide the merchant with the desired purchase order number, credit card number, or check information. In the preferred embodiment, the PDA device can either produce or verify additional physical identification, such as a digitally stored photo identification or biometric identification. For example, a PDA device could provide a merchant ID station with the owner's fingerprint, if the user of the PDA device doesn't have the same fingerprint the ID station could reject the transaction. A variation on this approach would have the PDA device provide the ID station with a preprogrammed personal identification number (PIN), if the user cannot match this PIN then the transaction may be voided. A photographic embodiment of the present invention allows the PDA device to send a digital image of the user to the ID station for the attendant to verify.

The present invention provides access control codes to multiple security outlets or service controllers through a PDA device. If the codes are accepted the digital device releases access to a requested resource. This release includes access to: desktop computers for boot up, selective computer data or programs, mechanical hardware such

as electronic doors, and service identification numbers such as credit card numbers and checking accounts. Additionally, one embodiment of the invention is a portable system which provides all file, user, network, or licensing authentication for a particular user.

Accordingly, it is a primary object of this invention to provide a system and method for coordinating the production of access control codes to access outlets or controllers using a PDA device. Other objects of the present invention include: providing a system and method for coordinating the production of access control codes that allows a user to access a secured digital device or an electronic readable file; providing a system and method for coordinating the production of access control codes that uses a control repository of information to collect access controls; providing a system and method for coordinating the production of access control codes that acts as a substitute for keys, cards, passwords, photographic, and biometric identification; and providing a system and method for coordinating the production of access control codes that interfaces with an external identification access card.

Additional objects and advantages of the invention will be set forth in the description which follows and in part will be obvious from the description, or may be learned by the practice of the invention. The objects and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly printed out in the appended claims. These and other objects and features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth herinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the manner in which the above-recited and other advantages and objects of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference to a specific embodiment thereof which is illustrated in the appended drawings. Understanding that these drawings depict only a typical embodiment of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 is a top level diagram of one embodiment of the present invention depicting access control for a computer;

Figure 2 is a flow chart of one embodiment of the present invention, illustrating access control at computer boot and login security;

Figure 3 is a flow chart of one embodiment of the present invention depicting access control used to secure computer files or e-mail;

Figure 4 is a flow chart of one embodiment of the present invention depicting access control requiring a PIN and/or photo identification; and

Figure 5 is a top level diagram of one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 provides an overview illustrating the use of a PDA device to control software and hardware access electronically connected to a digital device. A PDA 100 interfaces with an I.D. access card 102. The I.D. access card 102 may be in permanent, removable, or flexible communication with the PDA 100. A permanent connection is demonstrated by the addition of a chip which is installed within the PDA 100. The chip method has been established in other applications, but it has not been applied to PDA devices specifically in regards to access control or security features. If an IC chip is added to the PDA 100, the IC chip will have access to the PDA interfaces to the outside world through the PDA's processor. One embodiment would use the PDA's processor to read access numbers from the security chip and transmit the number to the device making the query. The querying device could then compare the transmitted number to its database to see if it was an acceptable number. Upon comparison of the devices the querying device could either accept or refuse access to its function e.g., building entry, computer access, transactional support, or purchasing.

Removable communication generally involves attaching the I.D. access card 102 to an interface on the PDA 100 for a limited time period to either download access control database or to program an access control extension. Examples would include serial cables, PDA cradles, hard coded memory cards, PCMCIA cards, disks, Wegand devices, or other encoding equipment. Once the I.D. access card 102 contacts the PDA 100, it provides either secured data structures or an encrypted I.D. database that can be verified later by local controller access points. One embodiment uses the I.D. access card 102 by attaching the card or similar device to the PDA 100 through a clip-on method. Appropriate hardware and software could be added so that when a query was made on the interface to the outside world, the PDA's processor would read the number from the security card and transmit to the device making the query. The querying device could authorize the PDA request based on a successful comparison of the transmitted number to the querying device's database. Examples of some PDA access control requests include: building entry, computer access, car entry, purchasing transactions, goods, etc.

Flexible connections can be created when no physical electronic contact is required between the I.D. access card 102 and the PDA 100, such as IR pulses, RF transmissions, Wegand devices, and wireless transceivers. Alternatively, the I.D. badge or clip-on PDA

interface previously mentioned, could function merely to hold the badge or I.D. card and not require the I.D. access card 102 to electronically interface with the PDA at all, just physically interface as a means of condensing and consolidating the access cards. In one variation of this non-interactive embodiment, the removal of the card or badge from the badge PDA interface either completely disables the PDA from functioning or limits operation of the PDA to a limited subset of the normal functions.

In addition to receiving information from an I.D. access card 102, the PDA interface devices can be used to facilitate communication between the PDA 100 and a digital device 108. Various PDA interface devices are employed to communicate with devices in the outside world including, but not limited to, the standard serial RS-232 port, a parallel port, an IR port, a PDA cradle connection, a RF bandwidth transceiver, Wegand device, magnetic coding or sensor, bar code reader, USB, wireless transceiver, and laser communication. Once an interface device is selected by the PDA 100, it can either interface with an I/O module 106 or with a PDA cradle 104. These interface input/output transceivers are in electronic communication with digital device 108. Once the digital device 108 has access to the PDA 100, it can verify whether access should be granted to a user for software access 110 or hardware access 112.

In one embodiment, special booting software is installed on a computer so that if the PDA device is not in the cradle, the computer can not be accessed. An access card code interface could also be used for protecting e-mail and communications between computers by requiring the PDA device to be in its cradle or near its receptor before access control would be allowed. This system would add security by controlling access to all things controlled or accessed by the PDA device, without requiring unnecessary security to impede the process. Various software access 110 features include inquiring whether the individual has approval to use licensed programs 114, whether approval exists to secured files 116, whether access should be granted to personal e-mail accounts 118, whether a specific user profile 120 should replace the standard desktop profile, and if a network profile 122 exists for a particular user. The network profile 122 could be stored on a central computer and, upon verification of a PDA 100 within an I/O cradle 108 at a particular digital device 108 access and rights and privileges to network, drives, data, and resources could be granted to the individual user, thereby allowing him to use local printers, fax machines, and other local facilities but also providing him with access to printers at his home location. In essence, the user would only need to plug his PDA 100 into I/O cradle 104 or interface with I/O module 106 to obtain personalized access throughout a company's LAN or WAN network.

In addition to software access 110, one of the significant features of the present invention is the ability to regulate hardware access 112. Hardware access 112 focuses primarily on boot control 124 of the digital device 108 and restrictive resource access to attached devices 126. By checking boot control 124, the digital device can determine whether the individual is even allowed to operate the machine. This feature is similar to utilizing a key, however, multiple digital codes could be utilized. Essentially, a traveler from another city could work on a computer at an out of town site and receive the authorization to boot the machine through his PDA. Whereas, a key required that a specific key be used on a specific machine, boot control 124 is applied to the entire computer network. Hardware access 112 also extends to attached devices 126 electrically linked or controlled by digital device 108. Attached devices 126 may include local printers, local modems, local network access, local e-mail access, local infra-red transceivers and various other attached devices like scanners, digital cameras, wireless links, main frame connections, etc.

Figure 2 is a flow chart that outlines how the PDA in a preferred embodiment can secure a computer at boot up or log in. Execution block 200 represents the restart or start of the computer. Execution block 202 requires that the computer look at the boot options stored in the boot sector or in the bootable prompt section. Decision block 204 determines whether the boot security bit is on. If the security bit in decision block 204 is not turned on, then protocol will jump immediately to execution block 216 and allow the computer to boot. If the bit is turned on, then decision block 206 queries whether the PDA is connected to the machine. If the PDA is not connected execution block 208 prompts the user to connect the PDA before proceeding further. If the PDA is connected, execution block 210 reads the identification code provided from the PDA. Decision block 212 determines whether or not an authorized I.D. is provided by the PDA device. If the correct device is not provided or the I.D. provided is not authorized access to this computer, execution block 214 does not allow the machine to boot. If the correct I.D. has been provided, execution block 216 allows the computer to boot as normal now that the access has been verified.

Figure 3 is a block diagram of an access control protocol that can be applied to software or hardware access. The access control protocol is initiated in execution block 300 whenever there is a request to access of an access control protocol that can be applied to software or hardware access. A protected software or hardware resource, such as e-mail or a protected file. At this point, a subprotocol initiates the security confirmation protocol which prevents the program from providing access or from loading further until the PDA has been verified. In decision block 302, the protocol discovers whether the

PDA is connected. If the authorized PDA is not connected, execution block 304 prompts the user to connected the appropriate PDA to the computer. Once the PDA is connected, execution block 306 exchanges of identification information. Decision block 308 determines whether the exchanged identification information is valid. If the information is valid, then execution block 310 allows access to the file, e-mail, or other computer software or hardware resource. If it is not valid, then the access control protocol ends without giving access to the file. This access control protocol allows users to access their files on a common computer shared with multiple users. E-mail files are optionally loaded directly down to the PDA once the identification authorization has been made. Additionally, a user could use a traveling work station in which he was only required to carry his PDA containing the appropriate identification information to request from the network server the user's standard desktop and access to the user's e-mail files. As a result, a traveler could go to a foreign office or another work site location, plug his PDA into the control port and be granted access to the computer with the same restrictions and limitations that he may have had at his workstation at home.

Figure 4 provides a flow chart depicting the use of a personal identification number (PIN) and photo identification to provide various commercial services or computer services. While these functions can be performed separately, this figure demonstrates how each layer can be chained together. For example, the PDA boot restriction depicted in figure 2 and the PDA attachment function in figure 3 could also e applied to figure 4 without deviating from the spirit of the invention. In fact such a chain represents one of the preferred embodiments. Execution block 400 requires the PDA to link to the identification station. Execution block 402 represents the identification station making a request for information from the PDA. Once this information has been provided, the decision block 404 determines if the PDA identification is correct. If it is not, the program will abruptly end and the user may be required to re-initialize. If the PDA identification is correct then the confirmation system could require in decision block 406 queries whether a PIN is required for use of this PDA I.D. number if no PIN is necessary with this PDA identification number. If a PIN is necessary, then execution block 408 requests a PIN from either the PDA or from the user through a user interface located on the I.D. station. Decision block 410 determines whether the PIN entered or received is valid. If the PIN is not valid, then decision block 414 prompts for the PDA to reconnect to determine whether another PIN should be attempted. If the PIN is valid, then a review of the requested service is made in execution block 412. Decision block 416 queries whether or not the requested services are available. If the services are not available then the session with the identification station

is terminated. If the requested services are available, then the execution block 418 will display a digital photo on the I.D. station for the individual running the station to verify identification. Alternatively, the digital photo may be directly displayed on the PDA. Decision block 420 may either query the operator of the I.D. station as to whether the photo check was valid or a digital camera may compare the images to authorize the user. If the photo check is valid, execution block 422 activates the requested available services. Some of the services that could utilize such a system include photo identification such as a drivers license, passport, video rental card, or credit card. This type of photo identification combined with access control date encryption provides a means for the PDA to replace a credit card. Using this system for commercial transactions allows for a paperless checking account where the account ledger would be automatically updated by the PDA. The PDA checking ledger could include detailed information about specific transactions where the data is received directly from the I.D. station. Medical records could also be carried on a PDA, thereby allowing the individual to provide complete medical records to each doctor that they visit, provide emergency personnel with vital information in an emergency situation, or provide patient access to their own medical records. This system of identification verification could also be used for ticketing on airlines, movies, concerts or similar transactions where funds are being transferred and verification of an individual might be necessary. And finally, a service that would be terribly useful for this system to perform is supplying selective access control to a building. Many of these implementations or embodiments could be incorporated using existing protocols and interfaces within the PDA.

Figure 5 provides a top level block diagram illustrating an access control embodiment useful in completing various transactions. PDA 500 interfaces with an I.D. access card 502. The I.D. access card 502 provides PDA authentication information 518, secured data structures 504, or enables the PDA to perform access control functions. The secured data structures 504, include: checking account information 506 and more specifically maintaining a checking ledger of checking balances based on checks authorized by the PDA; credit card or debit card information 508 also based on transactions approved by the PDA; and personal information 510 including contact information, medical records, academic records, and other relevant information; membership information 512 includes date structures containing official information such as driver's license identification, passport identification, club membership, and other activities. The membership information 512 is particularly conducive to the utilization of photographic identification and other means for biometric identification.

In one embodiment, security information is loaded or embedded into the PDA device 500 so that information about the person using the PDA device 500 is displayed in text or graphics on either the PDA screen or a controller screen for actual visual verification. The PDA device 500 with the proper access control information could be used as a credit card, interfacing through an infra-red (IR) port, serial port, wireless transceiver, or other communication device such as a magnetic card reader. The PDA device 500 being used as a credit card could keep track of expenditures made using the "new credit card." In essence, providing a real time check register balance for the credit card purchases.

The photo identification module is also used with official government verification documents such as a passport or drivers license. The sensitive nature of these documents requires that various security information be embedded within the transmitted access control codes. When being used in this manner, the PDA device 500 supplies the I.D. information for guaranteeing checks to a checkstand operator or I.D. station 516. The individual operating the checkregister or digital information collection device could receive the feedback from the PDA device 500 and verify that the individual providing the information was the authorized user. In this way, the PDA device 500 could not only provide verification but also act to write checks. For additional security, a PIN could be required for the individual to access the accounts stored on the PDA device 500.

PDA authentication 518 can occur in a variety of ways including matching a previously stored PIN 526, digitally stored photographic I.D. 524, and biometric fingerprint I.D. 528. A unique feature of the depicted embodiment is its method of verifying authentication. Previous systems require the processing of an attempted user's fingerprint in a central process or which would either have to compare the attempted user's fingerprint with hundreds or thousands of stored fingerprints in a database, or would received a user identification number key punched in by the person seeking access and then look up a database stored fingerprint corresponding to that code and make the comparison. Such a central lookup and comparison requires a great deal of central computer memory, processor power, and a secured data bus consisting of many conductor bus cables between each of the access control points and the central processor. As such, the authentication network requires either a considerable amount of time or a very high powered computer to complete the access control decision. This equipment and installation of the cables is terribly expensive, particularly when retrofitted to an existing building. A different approach to access control decision-making is implemented by the present invention depicted in figure 5. In the preferred embodiment, the PDA device 500 carries a biometric copy of the correct identifier's fingerprints in the PDA authentication

database 518. As such, the high security authentication comparison can be made directly at the access control station 516 by a processor located there. Thereby creating an access control system combining PDA device 500 functionality with user authentication so that only the authorized user or users may use that PDA device as an access control station 516. The access control station 516 can be a computer terminal, a computer file, a door, a check stand, a visa authorization point, a gate, or other situation wherein high security is desirable. In a preferred embodiment, the access control system includes a series of authentication codes or identification codes having encoded data stored within a PDA device database. In one form of the invention, user authentication involves a biometric feature such as a fingerprint of the intended user. The fingerprint is digitized, encoded and place in the PDA device database, preferably along with an encoded user identification number. An I.D. authentication reader at a high security access control station 516 includes a reader for the encoded data representing the encoded fingerprint, and also a fingerprint reader for reading the user's fingerprint at each instance of attempted access. Comparison of the attempted user's fingerprint with the stored fingerprint is preferably made directly at the access control station 516, so that only the access decision and a keyholder identification code as part of the encoded data need be sent to a central access processor. This occurs with the PDA 500 transmitting the fingerprint ID through the PDA interface 514 to the identification station 516. The user then places their finger on the identification station 516 and the fingerprint is compared with the transmitted fingerprint to obtain verification. A similar occurrence could occur with the PIN in that the PIN is transmitted from the PDA 500 through the PDA interface 514 to the I.D. station 516 which then accepts a PIN entered by the user to be compared to the stored PIN. The fingerprint I.D. and PINs can be located in secured data areas that can only be modified through the use of an I.D. access card 502 or through some other interface with the PDA 500. A decision to grant access affects the release of an electronic release or electronic strike, or electronic software hold. If desired, a right feature can be included into the system whereby each access control station 516 accessed or attempted to be accessed by a user will be recorded on the PDA device 500 providing for later reading of the PDA device to determine where access has been attempted. Additional records could be maintained through the authentication I.D. and access control process. Checking information 506 including checking account ledgers which could read new balances following the use by checking or a credit card debit card. Membership information 512 such as drivers license could contain previous convictions or other relevant information relating to the driver. Passport information could include visa information and other valuable traveling statistics. The medical information 510 could

contain previous accidents, surgeries, and medications that could be immediately accessible by medical personnel should an individual need to be treated for injuries and be in an unconscious or conscious state.

In a commercial transaction, once the access control station 516 has verified the identity of an individual, it can then access the secured data structures 504 from the PDA 500 and select an appropriate checking account information 506, credit card account information 508, personal information 510, or membership information 512 to provide to the goods or service provider 520 connected to the access control station 516. This, in essence, allows the user of the PDA 500 to only carry one device for multiple access control, a substantial improvement over the prior art. Controlling access to a building, or a car, is easily controlled using the PDA device 500 as the access control device.

The secure data structures 504 on the PDA device 500 could be expanded to have medical information for doctor visits, identification for libraries, ticketing of concerts, ski resorts, sporting events, flight reservations, car reservations, etc. The secure data structures 504 could be added to the PDA device 500 using an I.D. access card 502 as defined above, a write-once read-only memory chip, or using some type of file encrypting method to save the information entered by a government license division or similar agency. An additional security feature that could be added to the PDA device 500 would be a fingerprint reader that could be used to activate the PDA device I.D. functions. In this way, an individual could ensure that only his accounts were only accessed through his own biometric identification.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by United States Letters Patent is:

1. A method for authorizing access control to digital resources of a digital device using a person digital assistant (PDA), said method comprising of the steps of:

initializing a database controlled by said PDA with access control codes;

requesting access to said digital resources of said digital device;

relaying said access control codes upon request to said digital device;

selectively authorizing access by PDA to said digital resources based on said access control codes.

2. A method as recited in claim 1, where said digital resources include: licensed executable programs, secured data files, e-mail accounts, user profiles, network profiles, and attached peripheral devices.

3. A method as recited in claim 1, wherein said access control codes are automatically relayed between the digital device and the PDA when the PDA is electronically connected with at least one of a I/O cradle or an I/O module.

4. A method as recited in claim 3, wherein said I/O module comprises at least one of a serial port, a parallel port, an IR port, a PDA cradle connection interface, an RF transceiver, a Wegand interface, 2 magnetic sensor, a bar code render, a modem, a NIC, a USB, or 2 laser communication devices.

5. A method as recited in claim 1, further comprising the step of interfacing with an I.D. access card to enhance said database with specific access control codes.

6. A method as recited in claim 1, wherein the step of selectively authorizing access further comprises the step of authenticating a PDA user by receiving a verifying access code, said verifying access code including at least one of biometric identification scan, photographic identification, and personal identification number.

7. A method as recited in claim 1, where said database further comprises secured data structures, said secured data structures including at least one of checking account information, credit card information, personal information, membership information, medical information, and governmental identification information.

8. A method for authorizing access to a digital device using a personal digital assistant (PDA), said method comprising the steps of:

acquiring access information from an access module;

encoding access information into an identification data structure;

upon request and authorization, supplying identification data structure to a said digital device;

said digital device comparing the supplied identification data structure with approved access codes;

upon approval, enabling access.

9. A method as recited in claim 8, wherein the approved access codes are contained in an authorized user database.

10. A method as recited in claim 9, wherein the authorized user database is centrally located.

11. A method as recited in claim 9, wherein the authorized user database is maintained locally at a service controller site.

12. A method as recited in claim 8, wherein the decision to grant access affects the release of at least one of an electronic release, an electronic strike, an electronic software lock, a hardware lock, a digital device boot restriction, credit card information, personal information, medical information, and electronic commerce transactional information.

13. A method as recited in claim 12, further comprising the steps of

displaying a user dialog interface;

requesting a secondary verification from the user, said secondary verification including at least one of a personal identification number, biometric identification, photographic identification, a magnetic identification, and encoded identification codes.

14. An access control system using a PDA to selectively communicate identification codes for authorizing requested transactions, said apparatus comprising:

an access controller comprising:

(a) an access entrypoint for receiving information transmitted from said PDA and from a user,

(b) a controlled resource,

(c) an analysis module;

said PDA in communication with said access controller, said PDA comprising:

(a) a secure information database;

(b) an authentication database;

(c) an access controller interface.

15. The apparatus recited in claim 14, said access control system further comprising an I.D. access module, said I.D. access module comprising an encrypted I.D. database and a table of related verification codes;

said PDA further comprising an I.D. access module interface in at least one of flexible, removable, or attached communication with said I.D. access module.

16. The apparatus recited in claim 15, wherein said I.D. access module is removably attached to said PDA transmitting access information, said access information including at least one of access control codes, user information, and previous authorization attempts.

17. The apparatus recited in claim 14, wherein said secured data structures comprises information including at least one of checking account information, checking ledger balance, credit card information, debit card information, medical records, personal information, membership information, drivers license identification, and passport identification.

18. The apparatus recited in claim 14, wherein said PDA authentication database contains at least one of an external PIN, a biometric identification data structure, and a digital photographic identification.

19. The apparatus recited in claim 14, where said I/O interface further comprises an I/O selection module including an access I.D. card interface and an input/output interface such as a PDA device cradle.

20. A method for authenticating access requests to use digital resources of a digital device using a personal digital assistant (PDA), said method comprising the steps of:

electronically connecting said PDA to said digital device;

determining which security elements are active in conjunction with an access request for a requested digital resource, said security elements comprising at least one of a boot sector inhibitor, a digital resource restrictor, an external personal identification number (PIN) verifier, a digital photographic identification verifier, and a biometric identification authenticator;

collecting responses for required active security elements;

analyzing collected responses against an authorization database for the digital resource;

upon a match between said collected responses and said authorization database, allowing access to requested digital resource.

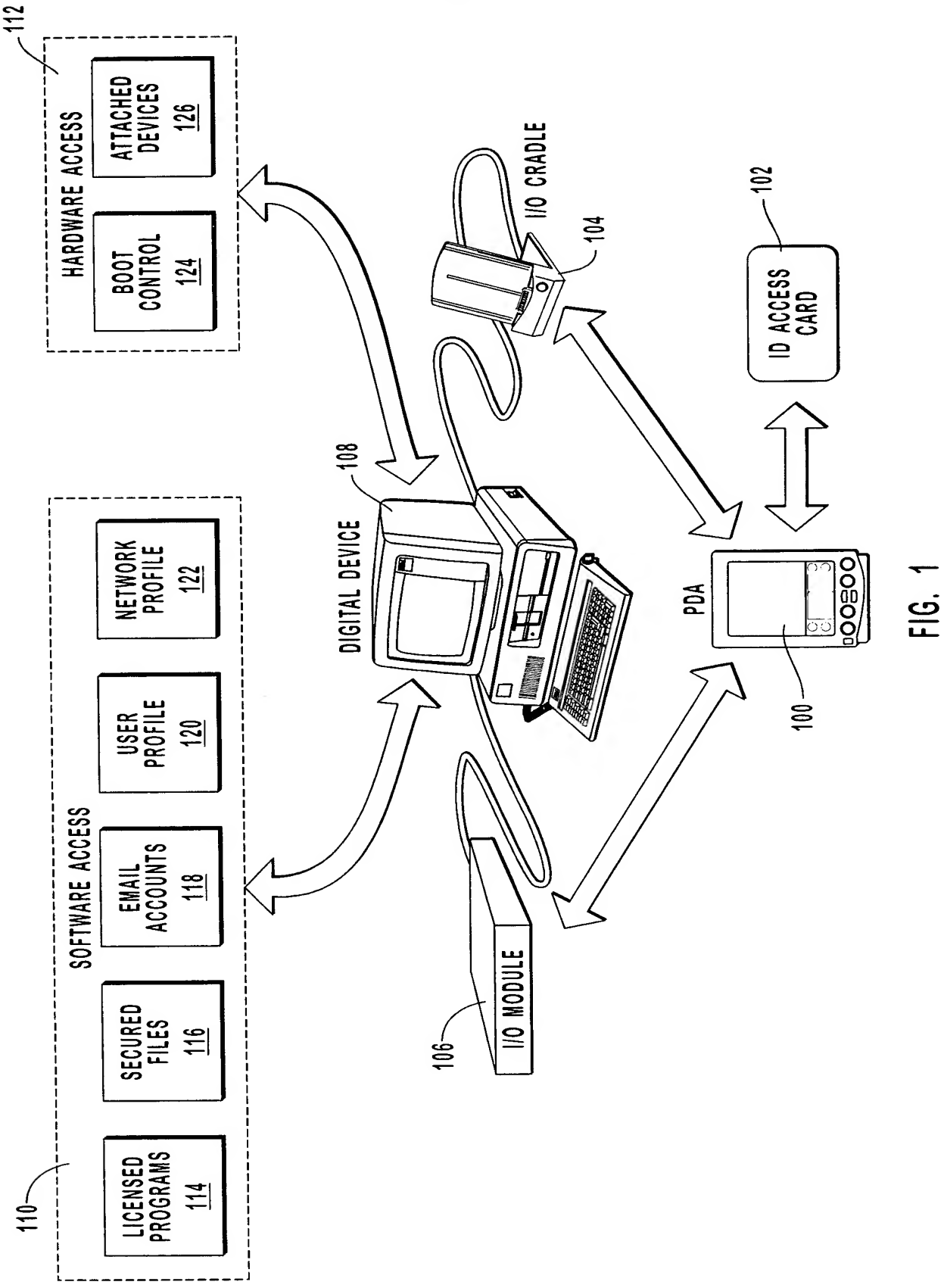

112
HARDWARE ACCESS
BOOT CONTROL 124
ATTACHED DEVICES 126
I/O CRADLE
104
102
ID ACCESS CARD
108
DIGITAL DEVICE
PDA
100
106
I/O MODULE
110
SOFTWARE ACCESS
LICENSED PROGRAMS 114
SECURED FILES 116
EMAIL ACCOUNTS 118
USER PROFILE 120
NETWORK PROFILE 122

FIG. 1

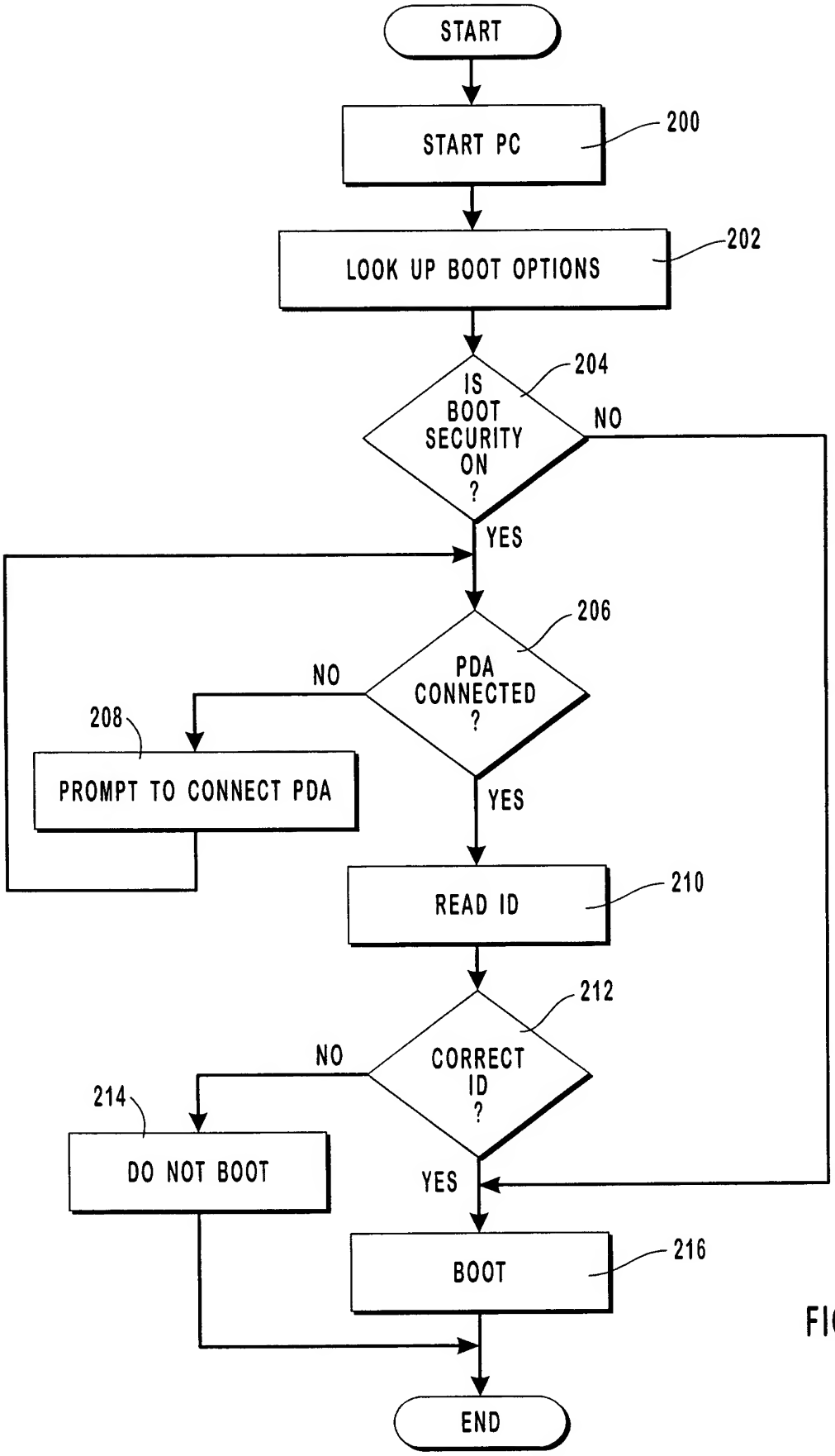

START
START PC
200
LOOK UP BOOT OPTIONS
202
IS BOOT SECURITY ON ?
204
NO
YES
PDA CONNECTED ?
206
NO
208
PROMPT TO CONNECT PDA
YES
READ ID
210
CORRECT ID ?
212
NO
214
DO NOT BOOT
YES
BOOT
216
END

FIG. 2

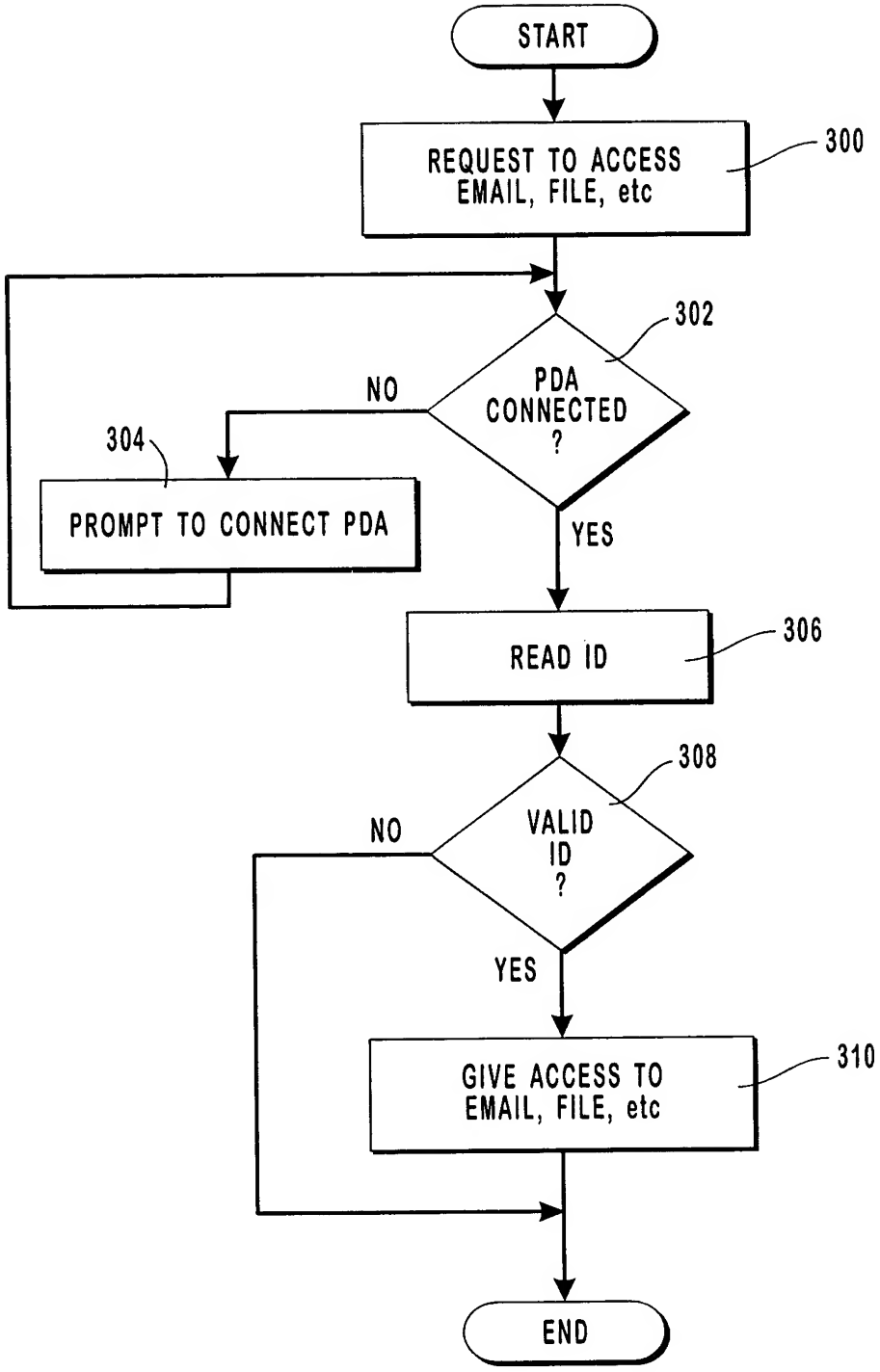

START
REQUEST TO ACCESS EMAIL, FILE, etc
300
302
PDA CONNECTED ?
NO
304
PROMPT TO CONNECT PDA
YES
READ ID
306
308
VALID ID ?
NO
YES
GIVE ACCESS TO EMAIL, FILE, etc
310
END

FIG. 3

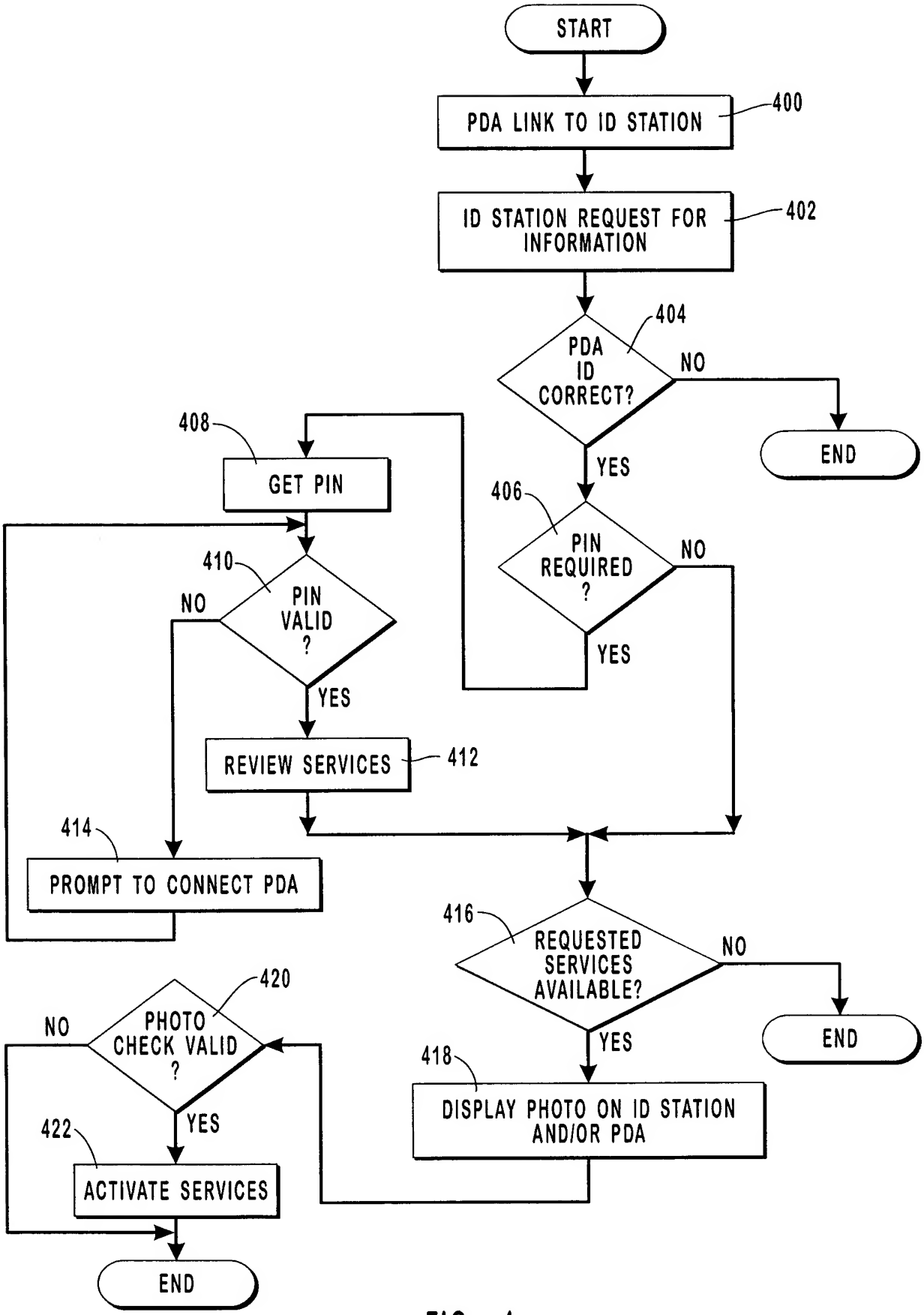

START
PDA LINK TO ID STATION
400
ID STATION REQUEST FOR INFORMATION
402
PDA ID CORRECT?
404
NO
END
YES
GET PIN
408
PIN REQUIRED ?
406
NO
YES
PIN VALID ?
410
NO
YES
REVIEW SERVICES
412
PROMPT TO CONNECT PDA
414
REQUESTED SERVICES AVAILABLE?
416
NO
END
YES
DISPLAY PHOTO ON ID STATION AND/OR PDA
418
PHOTO CHECK VALID ?
420
NO
YES
ACTIVATE SERVICES
422
END

FIG. 4

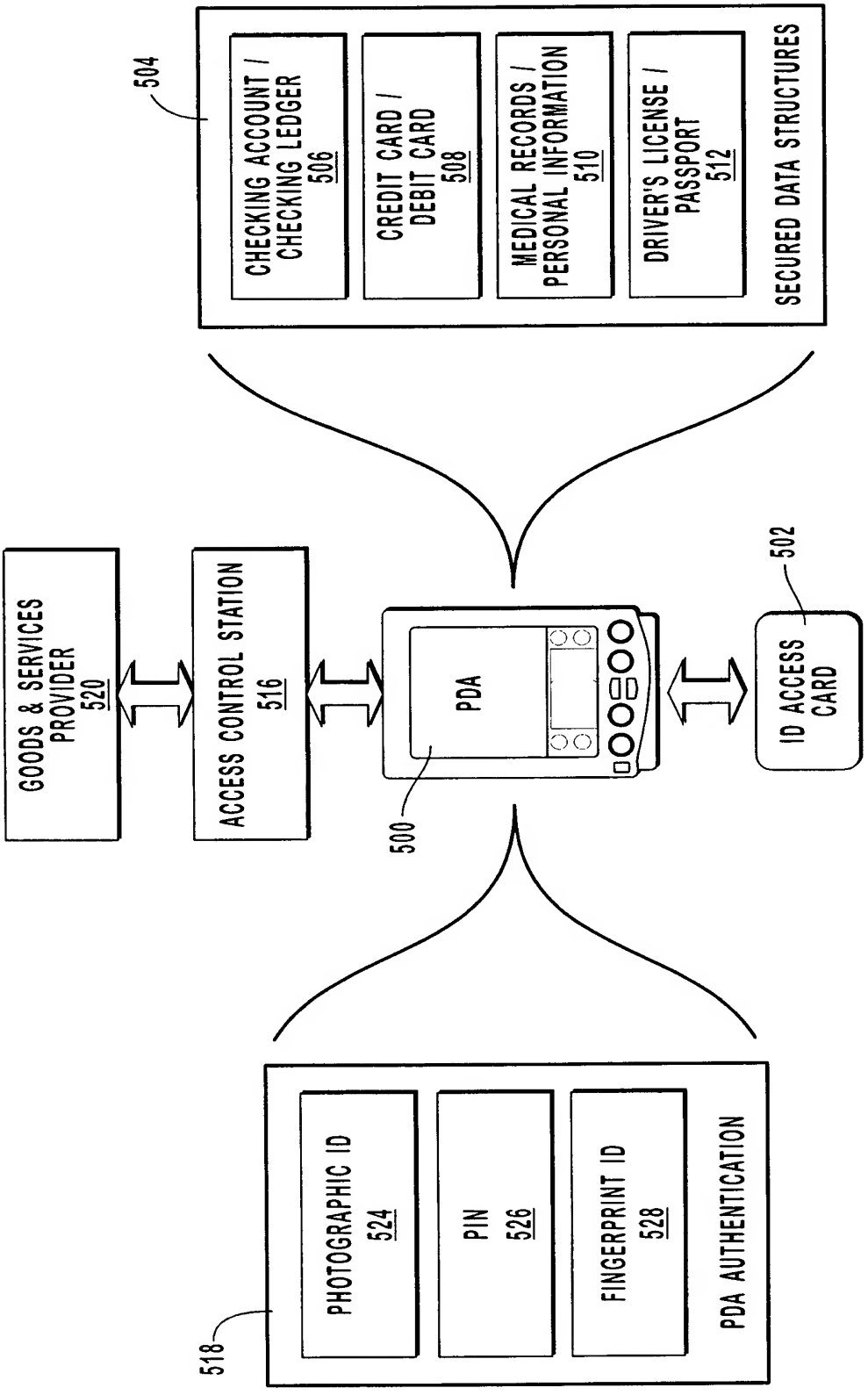

504
CHECKING ACCOUNT / CHECKING LEDGER 506
CREDIT CARD / DEBIT CARD 508
MEDICAL RECORDS / PERSONAL INFORMATION 510
DRIVER'S LICENSE / PASSPORT 512
SECURED DATA STRUCTURES
GOODS & SERVICES PROVIDER 520
ACCESS CONTROL STATION 516
PDA
500
ID ACCESS CARD
502
518
PHOTOGRAPHIC ID 524
PIN 526
FINGERPRINT ID 528
PDA AUTHENTICATION

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/28387

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/60

US CL : 705/50

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/50, 51, 55, 64, 65, 66, 67, 72, 73, 75, 76, 17, 41, 44; 235/380, 382; 713/152, 159, 168, 172, 184, 185, 186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 6,016,476 A (MAES et al) 18 January 2000 (18.01.2000), See entire document	1-20
A	US 5,781,723 A (YEE et al) 14 July 1998 (14.07.1998), See entire document	1-20
A	US 5,937,068 A (AUDEBERT) 10 August 1999 (10.08.1999), See entire document	1-20
A	US 5,475,375 A (BARRETT et al) 12 December 1995 (12.12.1995), See entire document	1-20
A	US 5,835,732 A (KIKINIS et al) 10 November 1998 (10.11.1998), See entire document	1-20
A,E	US 6,151,628 A (XU et al) 21 November 2000 (21.11.2000), See entire document	1-20
A,P	US 6,088,730 A (KATO et al) 11 July 2000 (11.07.2000), See entire document	1-20
A,P	US 6,105,008 A (DAVIS et al) 15 August 2000 (15.08.2000), See entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

07 December 2000 (07.12.2000)

Date of mailing of the international search report

09 JAN 2001

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

James Trammell James R. Matthews

Telephone No. (703)305-9700

Form PCT/ISA/210 (second sheet) (July 1998)